Critical infrastructure such as utilities and factories are monitored and operated via complex control systems. Idaho National Laboratory has pioneered thinking about "resilient" control systems that are more resistant to interruption from natural or man-made disasters.

Resilience as a way of life

By Dr. Craig Rieger and Dr. Ray Grosshans, *Idaho National Laboratory*

Hurricane Sandy bluntly reminded us how we take for granted the complex systems that provide energy, transportation, water, medical care, emergency response and security at levels considered luxurious just a generation ago. While utility providers and governmental agencies struggle to restore these vital services, it is worth contemplating the evolution of critical infrastructure systems.

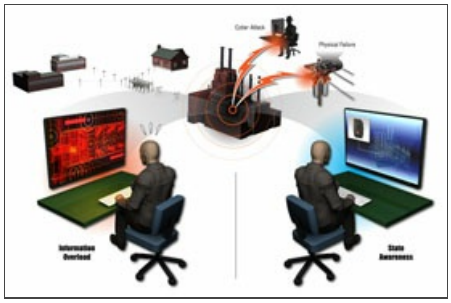
Idaho National Laboratory has pioneered thinking about "resilient" systems that are more resistant to interruption from natural or man-made disasters. Complex infrastructure systems with enhanced resilience have the capacity to maintain safe levels of operational normalcy in response to natural or man-made threats. INL has led the thinking about how to improve system resilience to minimize outages from unplanned natural disturbances, malicious attacks or new vulnerabilities inherent to smart grid systems.

INL's Instrumentation Controls and Intelligent Systems (ICIS) Distinctive Signature addresses the inherent fragilities that control systems must be able to cope with.

According to the National Academy of Engineering, the single most important engineering achievement of the 20th century was electrification as made possible by the electric grid. This ubiquitous grid, invisible to most consumers, includes over 9,200 electric generating units with more than 1 million megawatts of generating capacity connected to more than 300,000 miles of transmission lines. Always in the background, the grid has powered the nation's economy for more than 100 years, making possible innovations from the assembly line to the Internet.

Designed and constructed largely before microprocessors became widely available, the electric grid today suffers from underinvestment. The increasing number and duration of "brownouts" and "blackouts" over the past decade are the immediate consequences, as is the slow restart in the wake of Sandy.

The modern industrial plant control system is made up of numerous networked computer components, switches, valves and the like, which perform certain "smart" functions that control systems and operate processes. Such processes include refining hazardous chemicals, producing gasoline, or treating sewage. The success of these processes depends upon the quality of the engineering embedded in software and hardware systems and the technical expertise of those who operate plants to achieve process control.



Complex infrastructure systems with enhanced resilience can maintain safe levels of operational normalcy in response to natural or man-made threats. Click image to see larger version.

Modern control systems comprise interconnected parts, nodes and links, which collectively exhibit emergent properties or behaviors beyond those of individual components. Complexity in a system arises when component interdependencies supersede the function of individual components. These interdependencies can cause system rigidity or brittleness, which in turn leads to system failure when single elements fail or are intentionally compromised. The key problem is predicting, characterizing and resolving the component interactions in such a way that they cannot become common sources of failure.

INL has pioneered work to improve control system resilience. INL's Instrumentation, Control and Intelligent Systems distinctive signature has described two general ways that resilient systems cope with failure and attack: adaption or transformation. Adaptive systems include intelligent components designed to function in more than one role, allowing self-modification and leading to emergent properties that counterbalance anomalies while preserving function. Transformable systems utilize diversity to reconstitute into fundamentally new systems when external forces render an existing system indefensible. Ideally, evolutionary adaption and transformation are integrated in resilient systems.

Inherently resilient systems also can help protect control systems from malicious humans, i.e., "hackers." This is another area where INL is

contributing. Current control system security protections include layered "electronic gatekeepers" combined with security professionals employed as the last line of defense to recognize successful intrusions and thwart attacks. If security is defeated, co-opted computers become the soft underbelly of control systems. And the risk is growing: Implementing a so-called "Smart Grid" will deploy control systems that interact far more than current systems. Smart grids will manage inputs from both constant and intermittent energy sources while modulating outputs to achieve efficiency and economy by intelligently interacting with end user devices through advanced metering systems. Thus the potential vectors for cyberattack and access grow.

Through an interdisciplinary coalition with universities and industry, INL has invested in grand challenges and cutting-edge research to introduce resilience into control system designs. Recognition of the hard problems that must be addressed in an interdisciplinary fashion have inspired several years of an international symposium on resilient systems and a technical committee to codify principals and standards. The outcomes of these initiatives will affect how future generations of system designers approach next-generation designs to ensure they are inherently resilient.

INL has led the thinking to improve system resilience and minimize outages from natural disturbances, attacks or vulnerabilities inherent to smart grid systems.

Notwithstanding the engineering achievements embodied in our advanced critical infrastructures, maintaining normalcy in the face of malicious attacks and unexpected threats such as Hurricane Sandy remains a challenge. Addressing this challenge will require resilient control system technologies that adapt and transform in real time to both failures and attacks. Truly resilient systems intelligently route around broken system components to avoid cascading failures. Resilient systems draw on reserve resources to sustain life-safety systems. And resilient systems focus human attention on the problems machines either can't or shouldn't solve alone.

The development of such technologies will underpin next-generation designs for critical infrastructure, including chemical plants, refineries, nuclear facilities and defense systems, the failure of which causes even greater risk than the loss of use.

(*Posted Jan. 22, 2013*)

Feature Archive